FIG.1

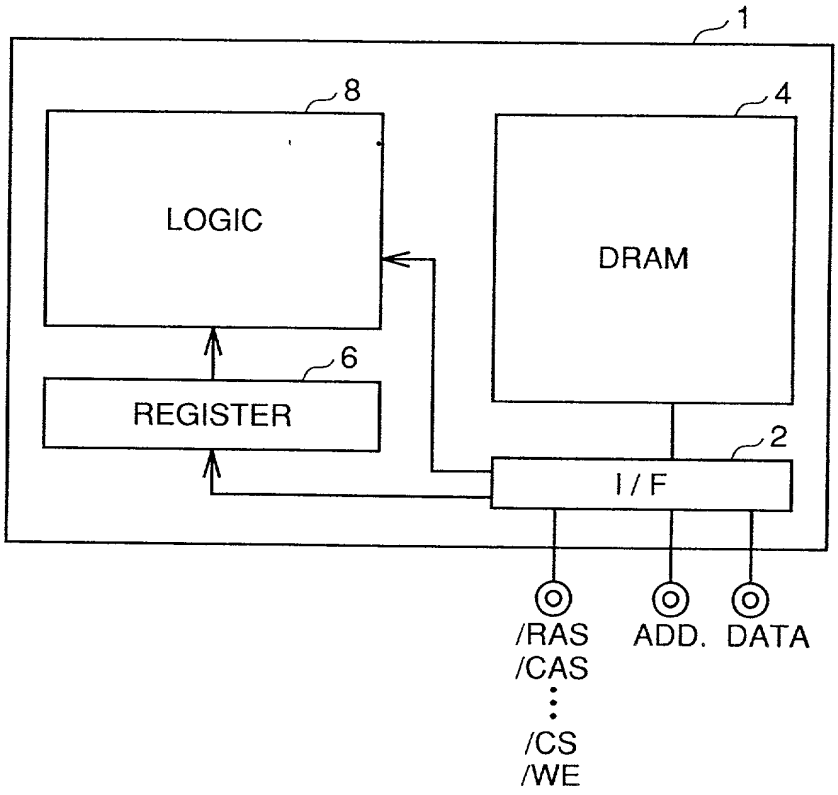

1
8
LOGIC
4
DRAM
6
REGISTER
2
I / F
/RAS
/CAS
/CS
/WE
ADD.
DATA

FIG.2

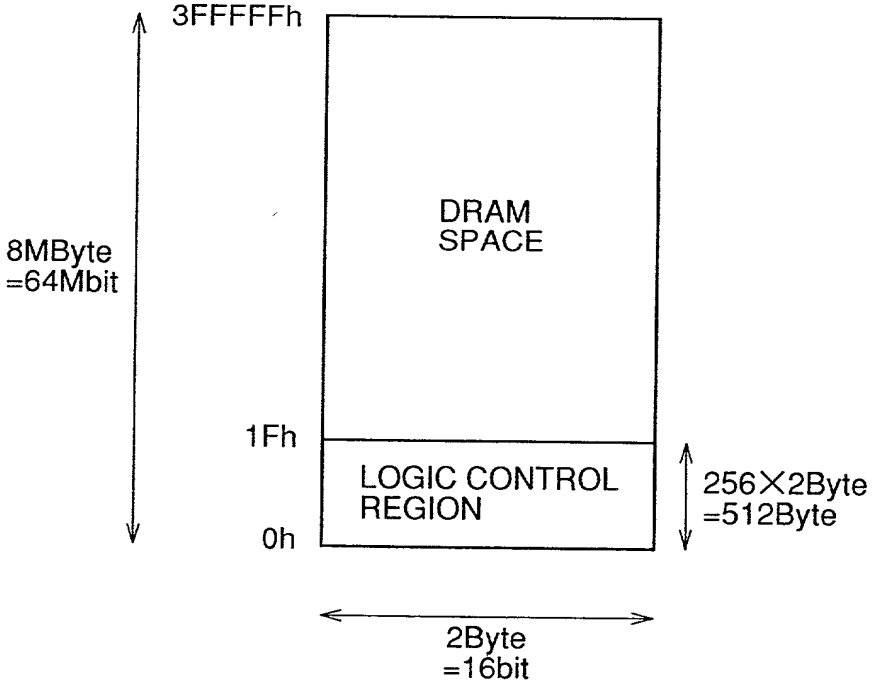

3FFFFFh
8MByte
=64Mbit
DRAM
SPACE
1Fh
LOGIC CONTROL
REGION
0h
256×2Byte
=512Byte
2Byte
=16bit

FIG.3

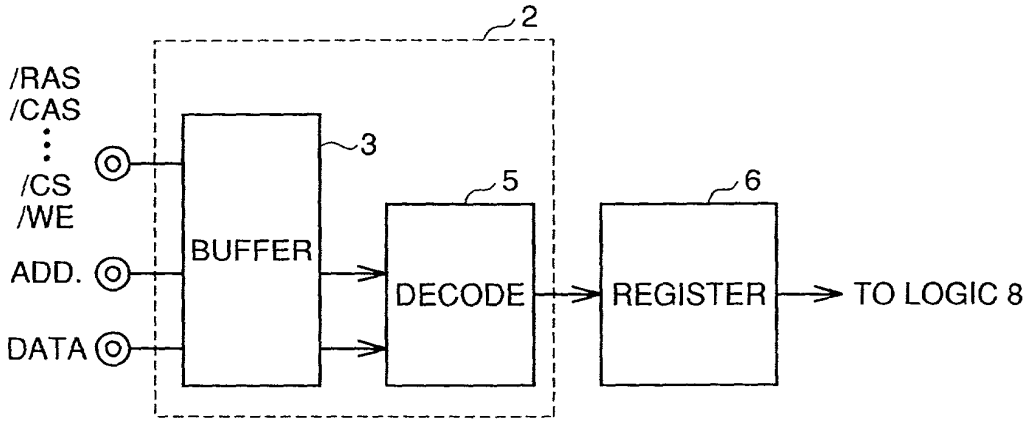


FIG.4

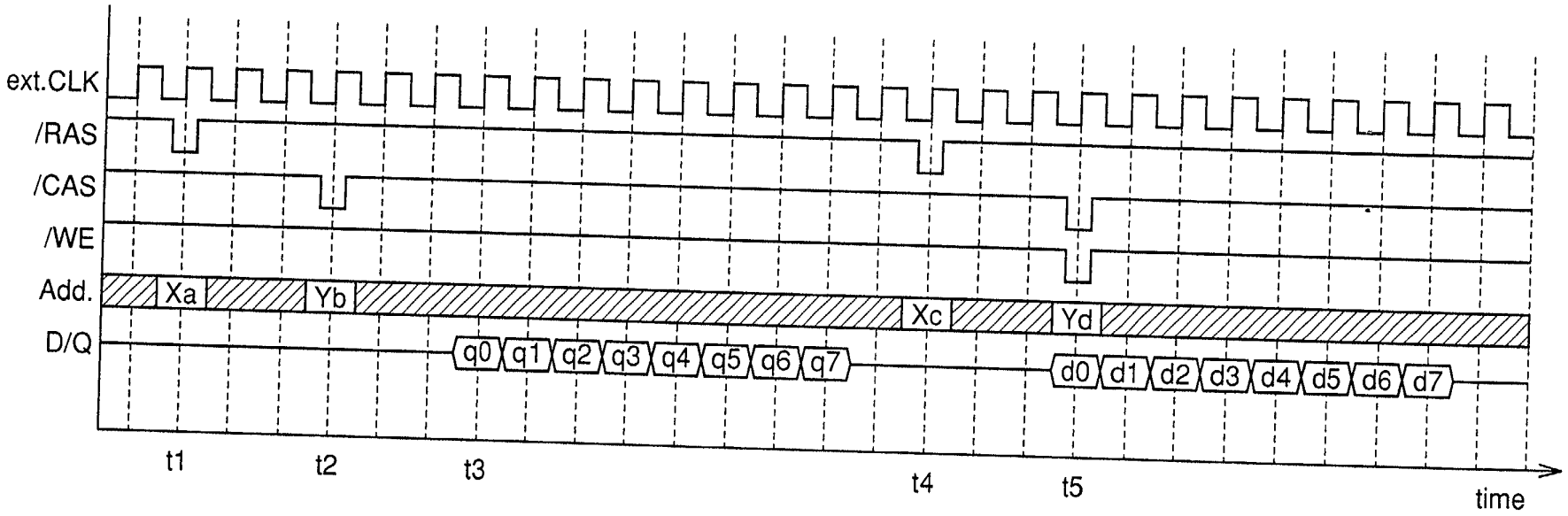

ext.CLK
/RAS
/CAS
/WE
Add.
D/Q
Xa
Yb
Xc
Yd
q0
q1
q2
q3
q4
q5
q6
q7
d0
d1
d2
d3
d4
d5
d6
d7
t1
t2
t3
t4
t5
time

FIG.5

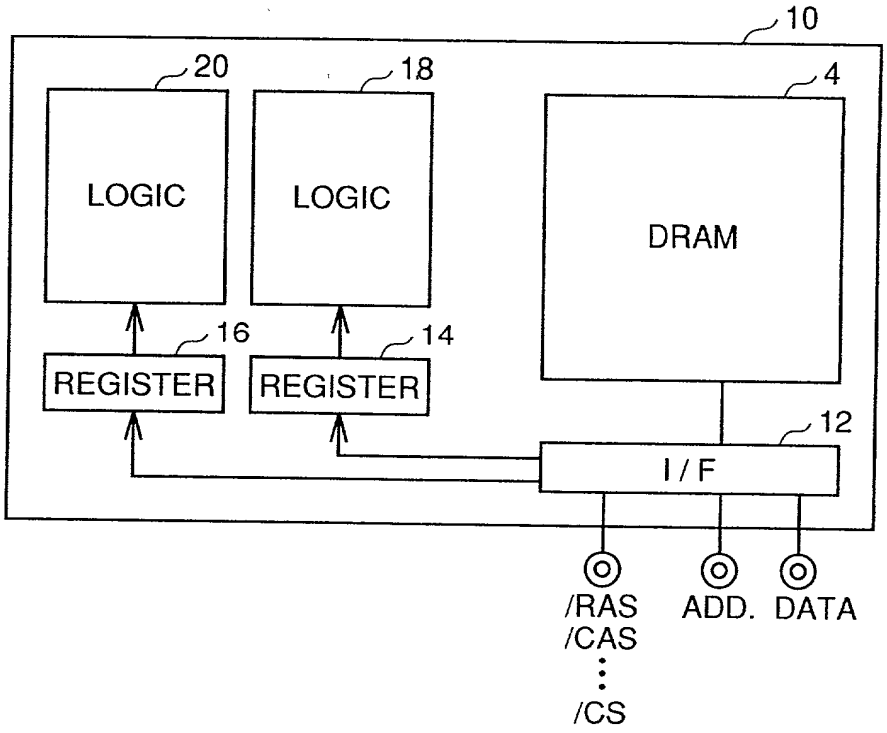

10
20
18
4
LOGIC
LOGIC
DRAM
16
14
REGISTER
REGISTER
12
I / F
/RAS
/CAS
/CS
ADD.
DATA

FIG.6

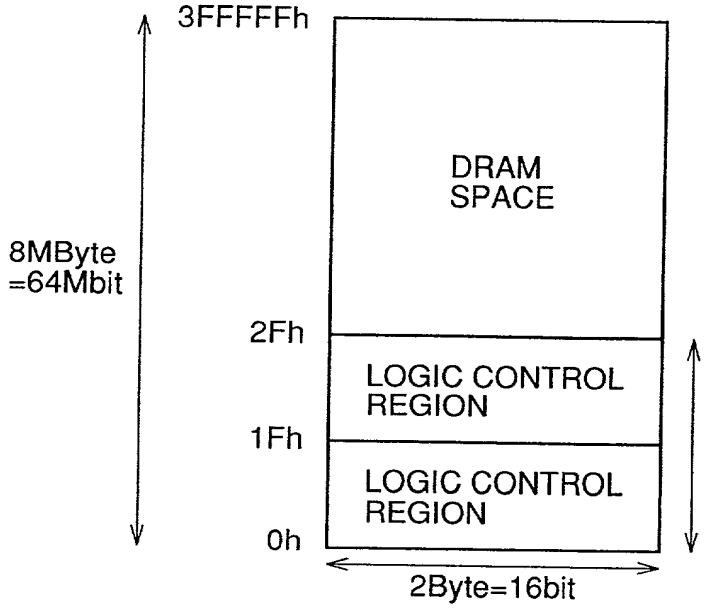

3FFFFFh
DRAM
SPACE
8MByte
=64Mbit
2Fh
LOGIC CONTROL
REGION
1Fh
LOGIC CONTROL
REGION
0h
2Byte=16bit

FIG.7

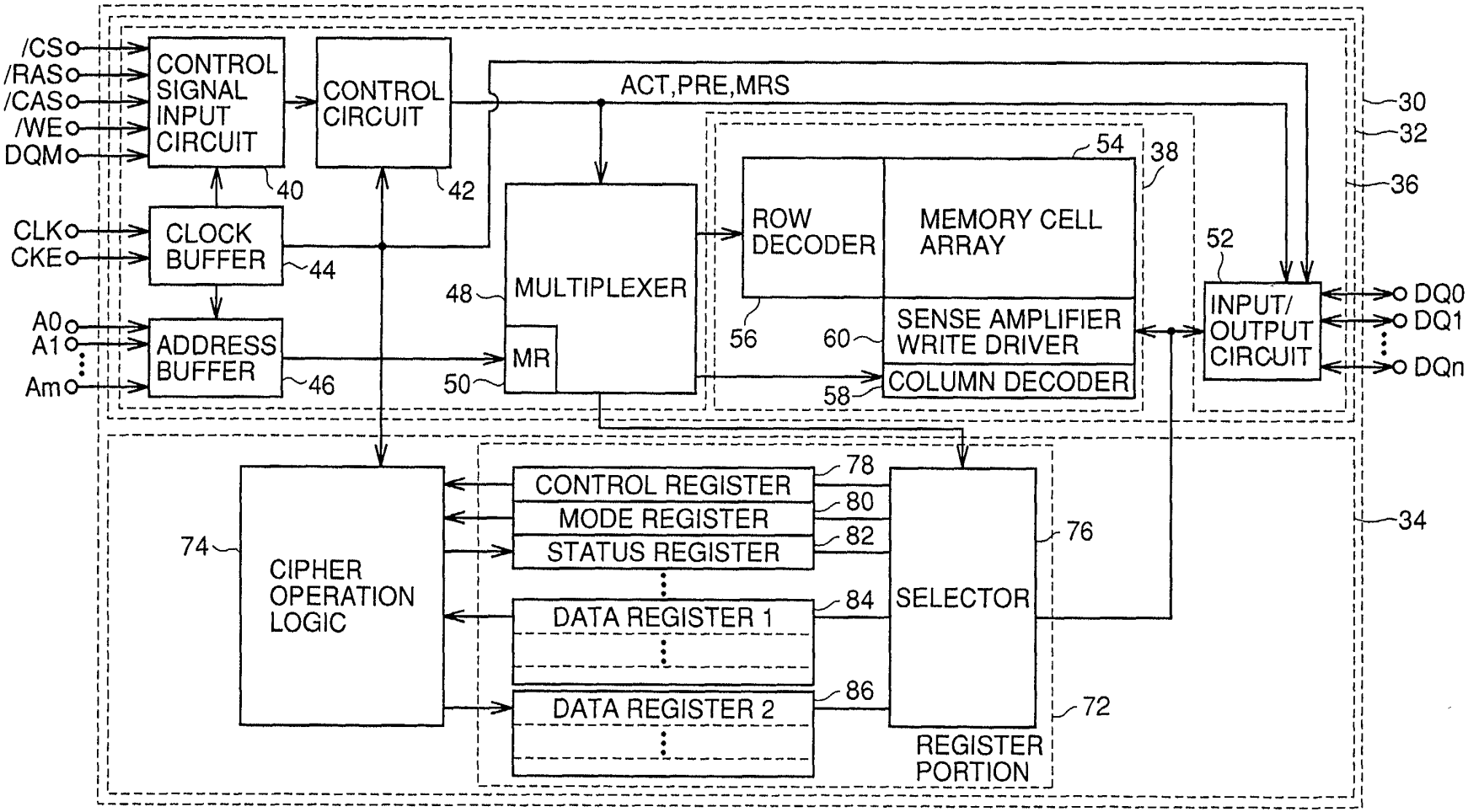

/CS
/RAS
/CAS
/WE
DQM
CONTROL SIGNAL INPUT CIRCUIT
40
CONTROL CIRCUIT
42
ACT,PRE,MRS
30
32
36
CLK
CKE
CLOCK BUFFER
44
A0
A1
Am
ADDRESS BUFFER
46
48
MULTIPLEXER
MR
50
54
38
ROW DECODER
MEMORY CELL ARRAY
56
60
SENSE AMPLIFIER WRITE DRIVER
58
COLUMN DECODER
52
INPUT/ OUTPUT CIRCUIT
DQ0
DQ1
DQn
74
CIPHER OPERATION LOGIC
78
CONTROL REGISTER
80
MODE REGISTER
82
STATUS REGISTER
84
DATA REGISTER 1
86
DATA REGISTER 2
SELECTOR
76
72
REGISTER PORTION
34

FIG.8

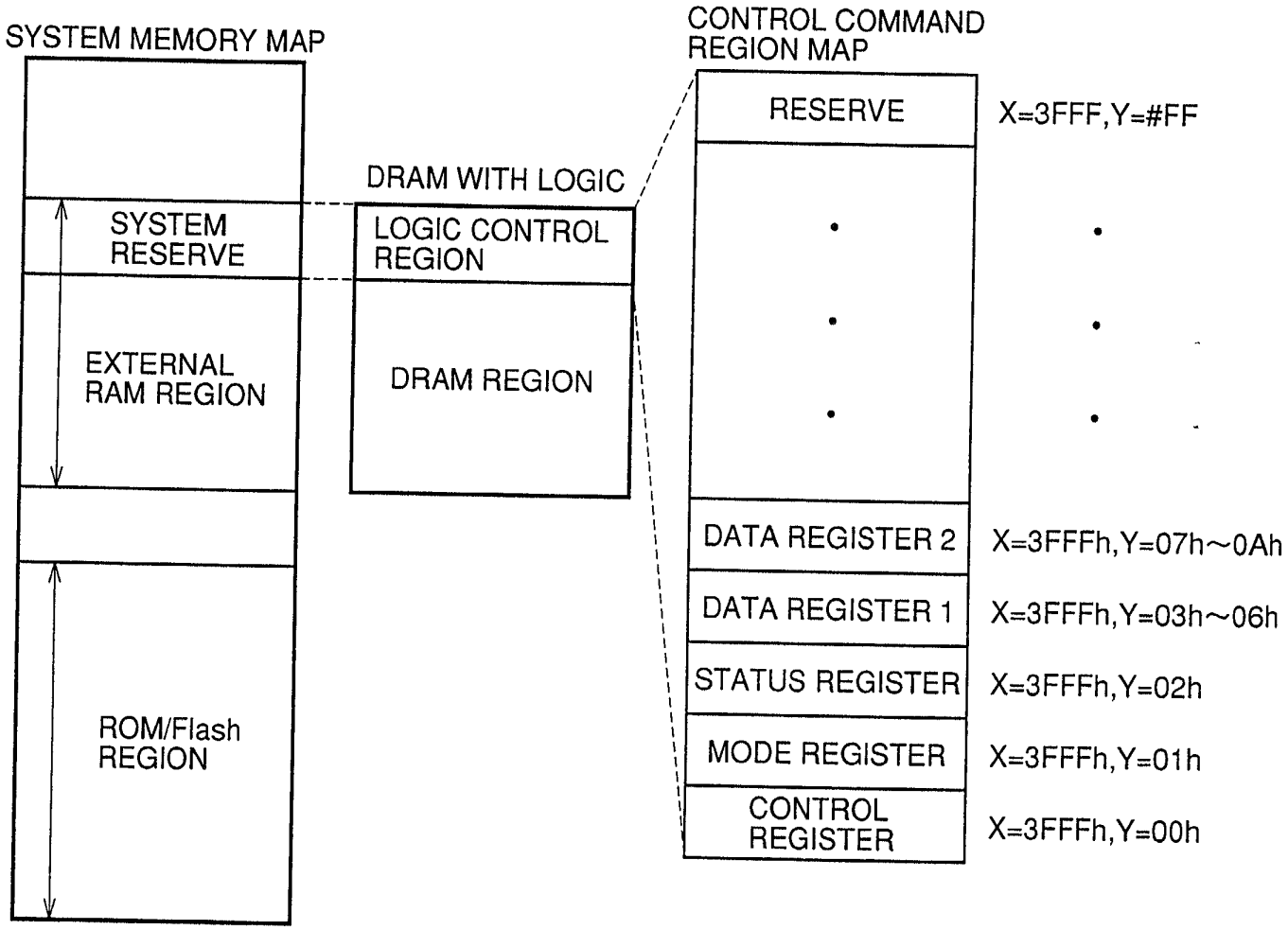

SYSTEM MEMORY MAP
SYSTEM RESERVE
EXTERNAL RAM REGION
ROM/Flash REGION
DRAM WITH LOGIC
LOGIC CONTROL REGION
DRAM REGION
CONTROL COMMAND REGION MAP
RESERVE
X=3FFF,Y=#FF
DATA REGISTER 2
X=3FFFh,Y=07h~0Ah
DATA REGISTER 1
X=3FFFh,Y=03h~06h
STATUS REGISTER
X=3FFFh,Y=02h
MODE REGISTER
X=3FFFh,Y=01h
CONTROL REGISTER
X=3FFFh,Y=00h

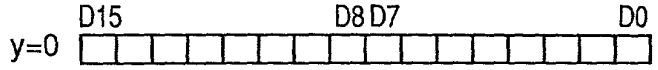
FIG.9

PUBLIC KEY CRYPTOSYSTEM	SECRET KEY CRYPTOSYSTEM	
		BLOCK ENCRYPTION MODE
RSA	DES Triple DES	ECB:Electric Code Book CBC:Cipher Block Chaining OFB:Output Feed Back CFB:Cipher Feed Back

SUPPORTED CRYPTOSYSTEMS

FIG.10

- BOTH FOR PUBLIC KEY AND SECRET KEY METHODS

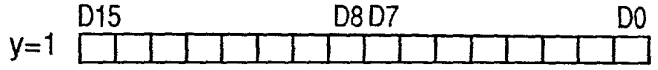


D0 =1: CIPHER FUNCTION RESET

D1 =1: FLAG INDICATING CIPHER PROCESS
(ACCESS AFTER 0 IS VERIFIED)

FIG.11

- CONTROL IN SECRET KEY METHOD

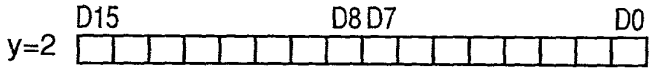


D1,0=01/10/00: DES/Triple DES/HOLD
(SELECT ENCRYPTION METHOD,
INHIBIT OTHER COMBINATIONS)

D5-2=0001/0010/0100/1000/0000: ECB/CBC/OFB/CFB64/HOLD
(SELECT BLOCK ENCRYPTION MODE,
INHIBIT OTHER COMBINATIONS)

D8-6=001/010/100/000: Normal/Block/Buffer/HOLD
(DATA PROCESSING MODE,
INHIBIT OTHER COMBINATIONS)

FIG.12

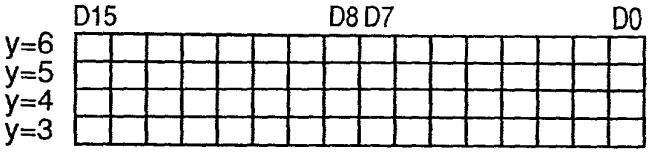


D1,0=01/10/00: ENCRYPTION/DECRYPTION/HOLD
(11 REPRESENTS INHIBIT)

D5,4=01/10/00: START/STOP/HOLD OF INPUT OF PLAIN TEXT
OR CRYPTOGRAM
(11 REPRESENTS INHIBIT)

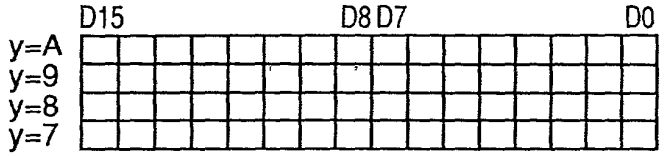
D9-6=1000-0001/0000: TEXT LENGTH (BYTE UNIT)/HOLD IN ONE BLOCK
OF OFB, CFB
(INHIBIT OTHER COMBINATIONS)

FIG.13



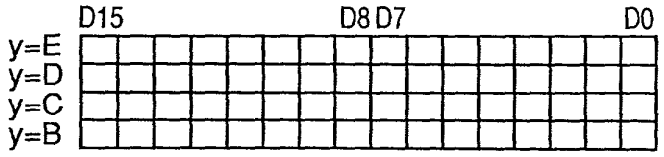
KEY 1 (MAXIMUM LENGTH OF 64 BITS): KEY OF DES,
KEY WITH RESPECT TO E OF EDE OF TRIPLE DES

FIG.14



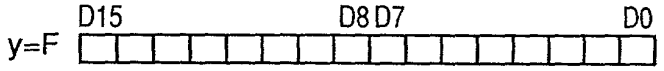
KEY 2 (MAXIMUM LENGTH OF 64 BITS):
KEY WITH RESPECT TO D OF EDE OF TRIPLE DES

FIG.15



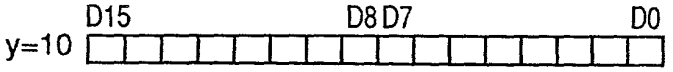
IV: INITIAL VECTOR

FIG.16



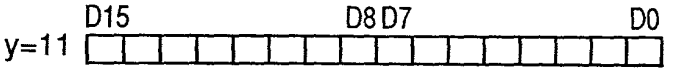
BLOCK LENGTH: SET BY BYTE UNIT
Max=2kByte(D=#FF) Min=1Byte(D=#0)

FIG.17



BUFFER NUMBER: VALID IN BUFFER MODE
Max=64k(D=#FFFF) Min=1(D=#0)

FIG.18



BUFFER ID:

FIG.19

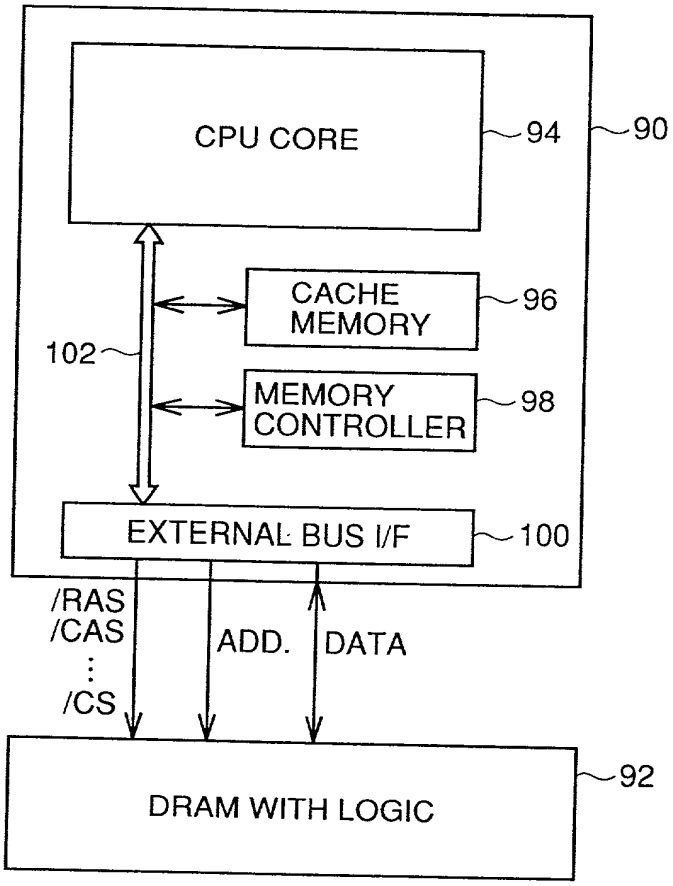

CPU CORE
94
90
CACHE MEMORY
96
102
MEMORY CONTROLLER
98
EXTERNAL BUS I/F
100
/RAS
/CAS
/CS
ADD.
DATA
DRAM WITH LOGIC
92

FIG.20

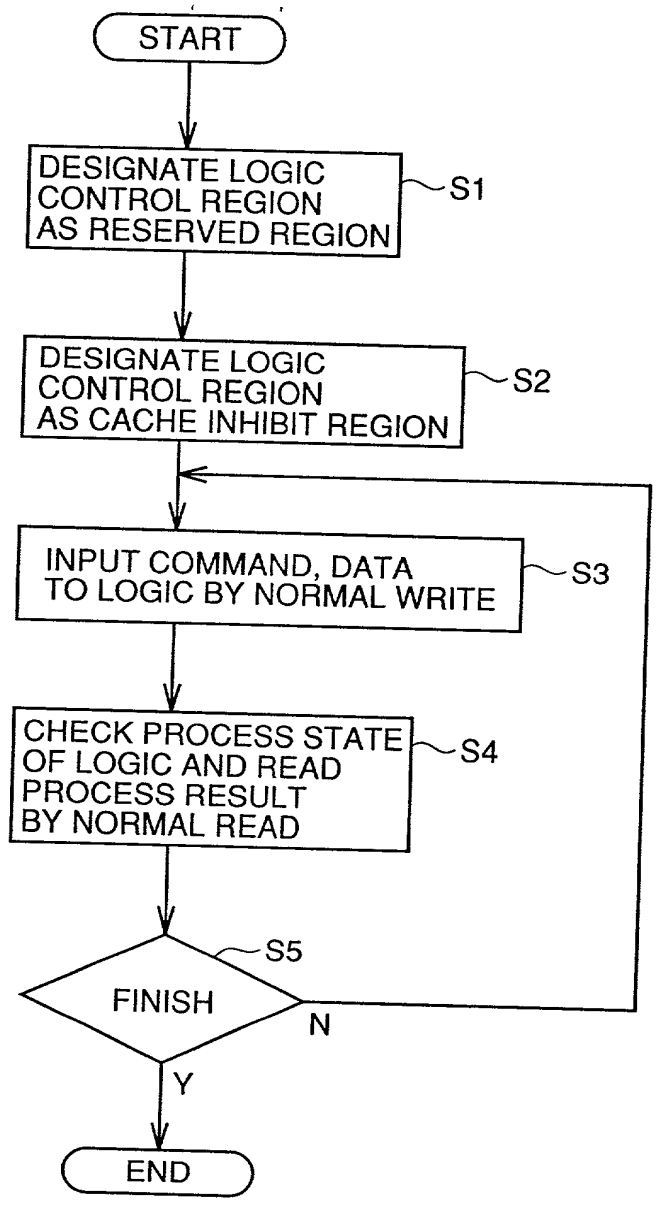

START
DESIGNATE LOGIC CONTROL REGION AS RESERVED REGION
S1
DESIGNATE LOGIC CONTROL REGION AS CACHE INHIBIT REGION
S2
INPUT COMMAND, DATA TO LOGIC BY NORMAL WRITE
S3
CHECK PROCESS STATE OF LOGIC AND READ PROCESS RESULT BY NORMAL READ
S4
S5
FINISH
N
Y
END

FIG.21

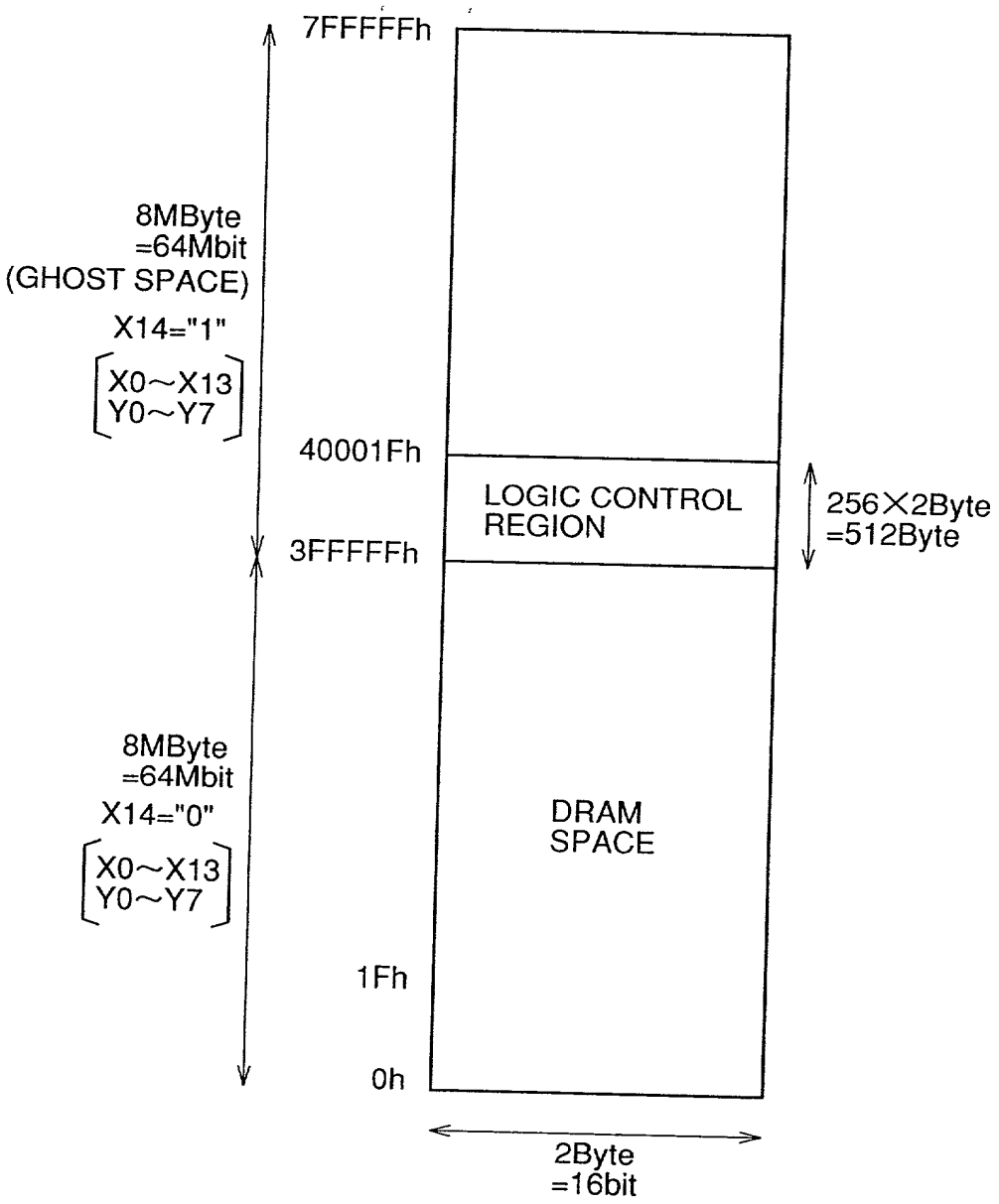

7FFFFFh
8MByte
=64Mbit
(GHOST SPACE)
X14="1"
X0~X13
Y0~Y7
40001Fh
LOGIC CONTROL
REGION
256×2Byte
=512Byte
3FFFFFh
8MByte
=64Mbit
X14="0"
X0~X13
Y0~Y7
DRAM
SPACE
1Fh
0h
2Byte
=16bit

FIG.22

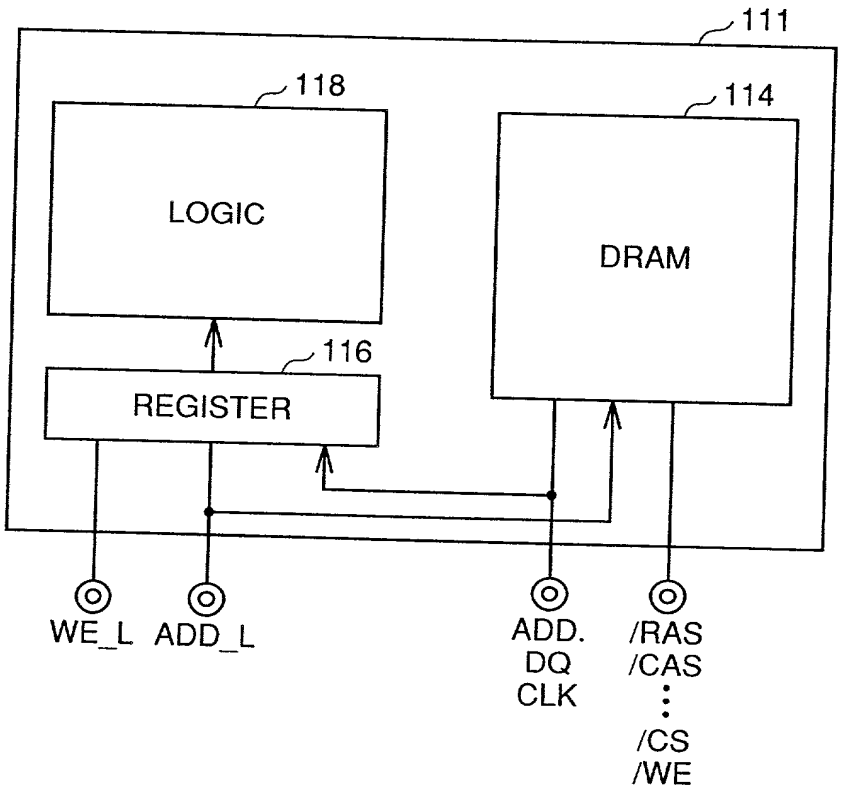

111
118
LOGIC
114
DRAM
116
REGISTER
WE_L
ADD_L
ADD.
DQ
CLK
/RAS
/CAS
/CS
/WE

FIG.23

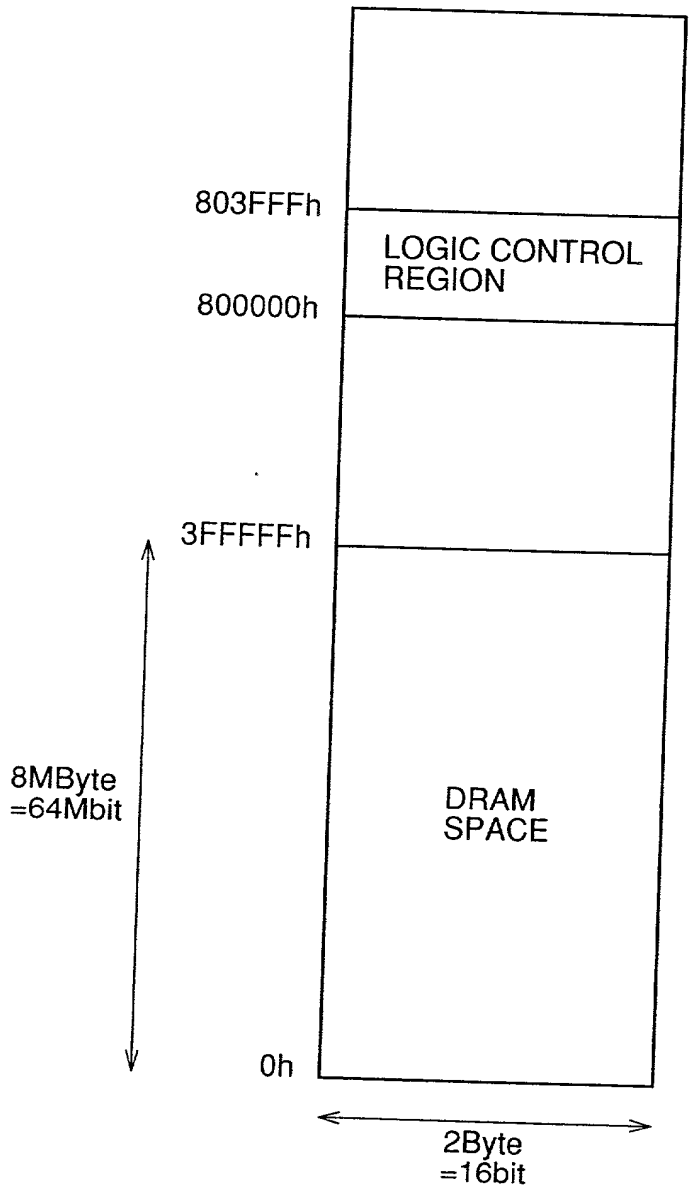

803FFFh
LOGIC CONTROL REGION
800000h
3FFFFFh
8MByte
=64Mbit
DRAM SPACE
0h
2Byte
=16bit

FIG.24

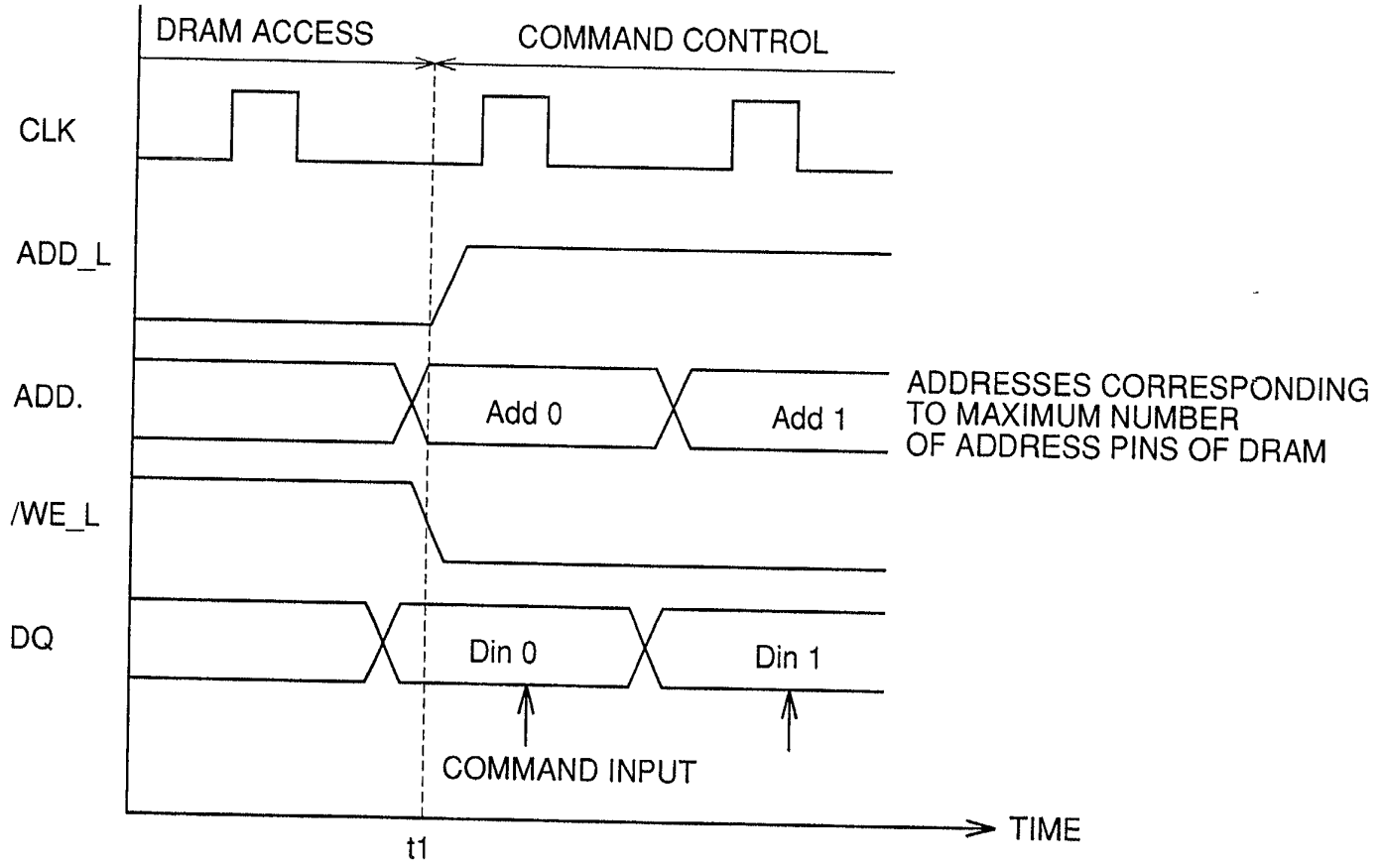

DRAM ACCESS
COMMAND CONTROL
CLK
ADD_L
ADD.
Add 0
Add 1
ADDRESSES CORRESPONDING
TO MAXIMUM NUMBER
OF ADDRESS PINS OF DRAM
/WE_L
DQ
Din 0
Din 1
COMMAND INPUT
TIME
t1

FIG.25

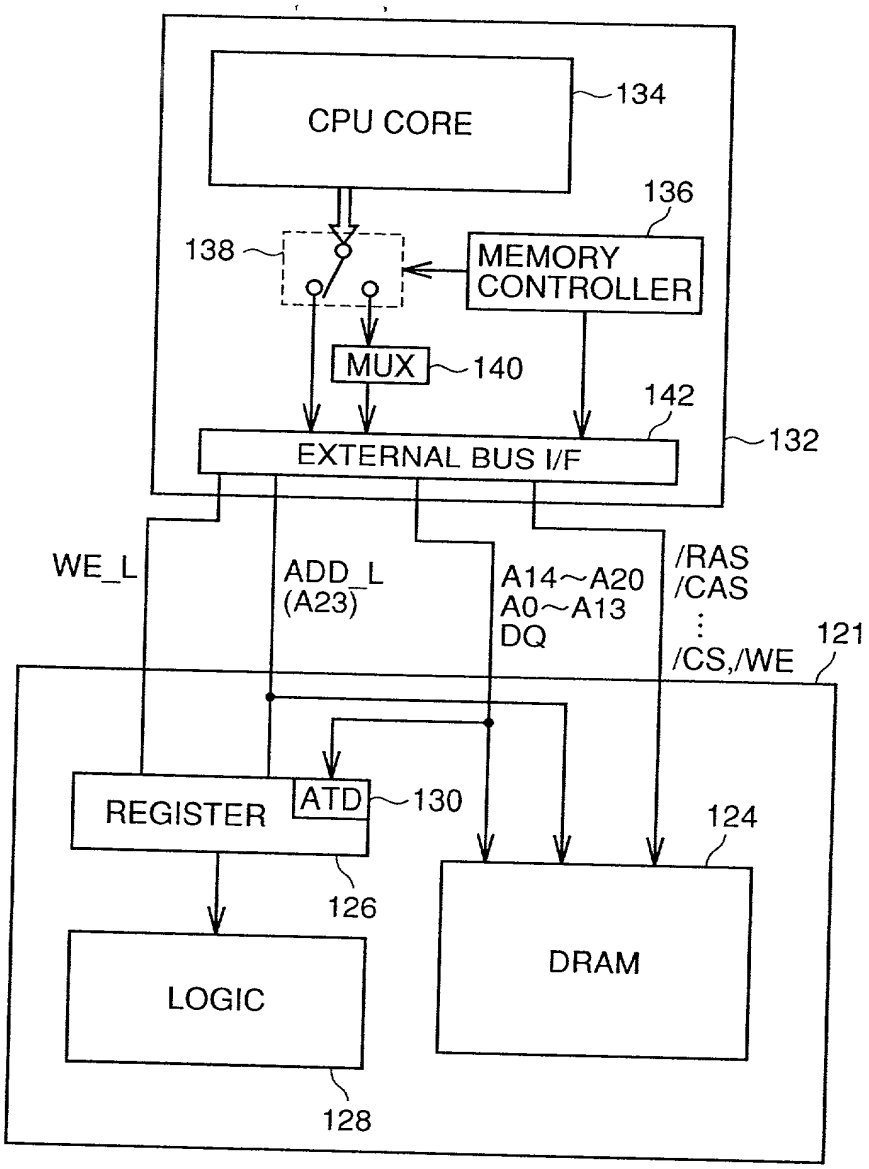

CPU CORE
134
136
138
MEMORY CONTROLLER
MUX
140
142
EXTERNAL BUS I/F
132
WE_L
ADD_L
(A23)
A14~A20
A0~A13
DQ
/RAS
/CAS
/CS,/WE
121
REGISTER
ATD
130
124
126
LOGIC
DRAM
128

FIG.26

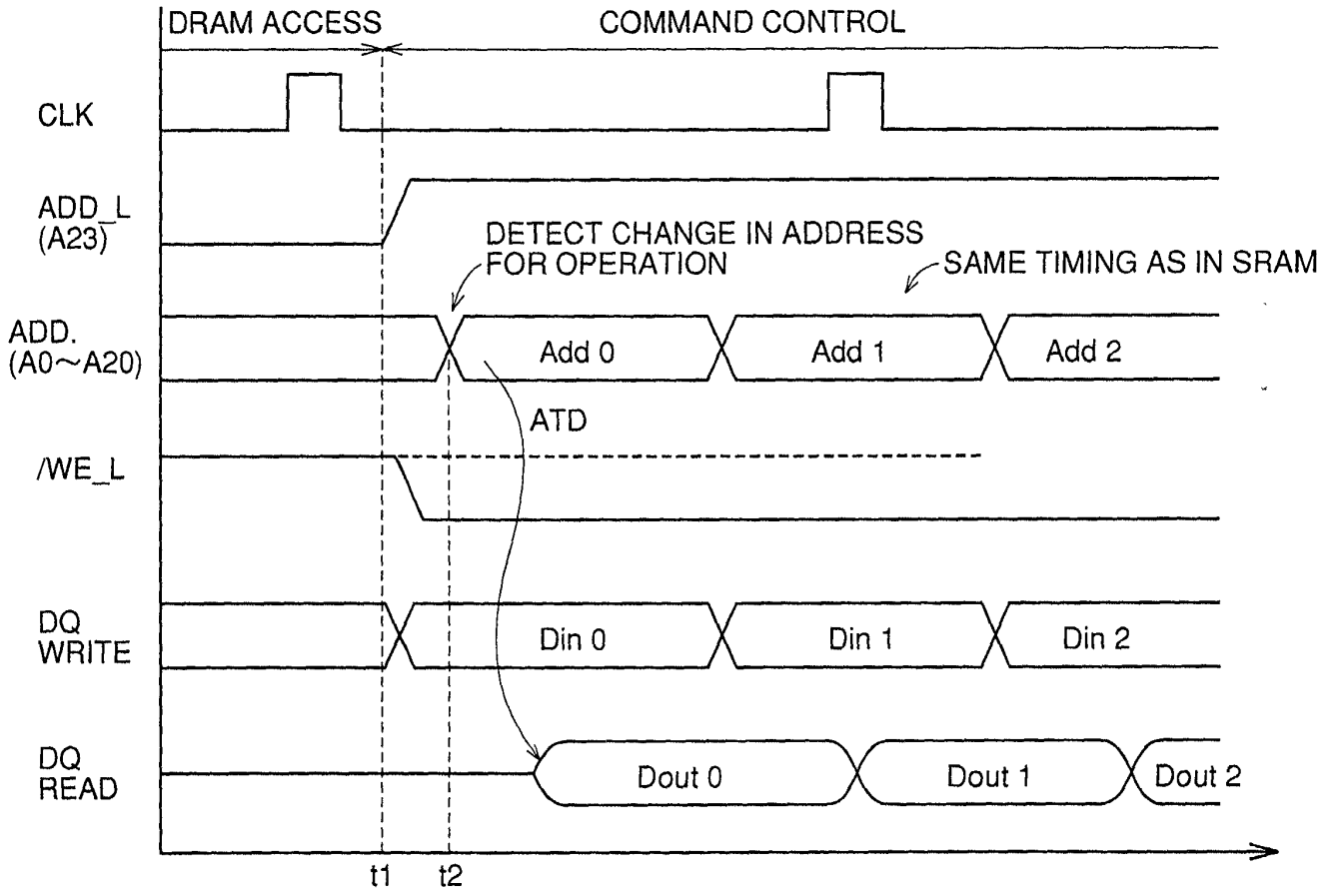

DRAM ACCESS
COMMAND CONTROL
CLK
ADD_L
(A23)
DETECT CHANGE IN ADDRESS
FOR OPERATION
SAME TIMING AS IN SRAM
ADD.
(A0~A20)
Add 0
Add 1
Add 2
ATD
/WE_L
DQ
WRITE
Din 0
Din 1
Din 2
DQ
READ
Dout 0
Dout 1
Dout 2
t1
t2

FIG.27

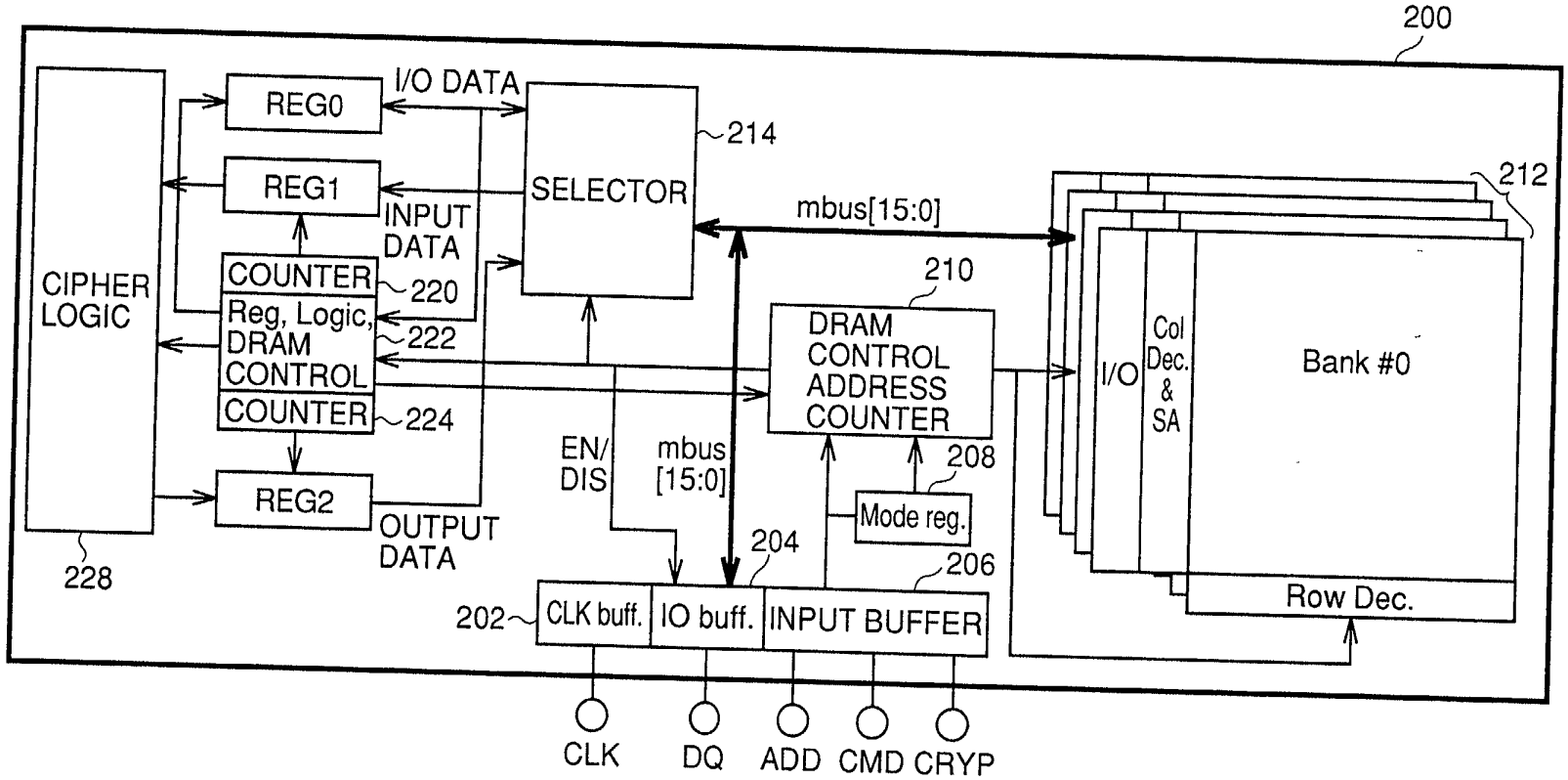
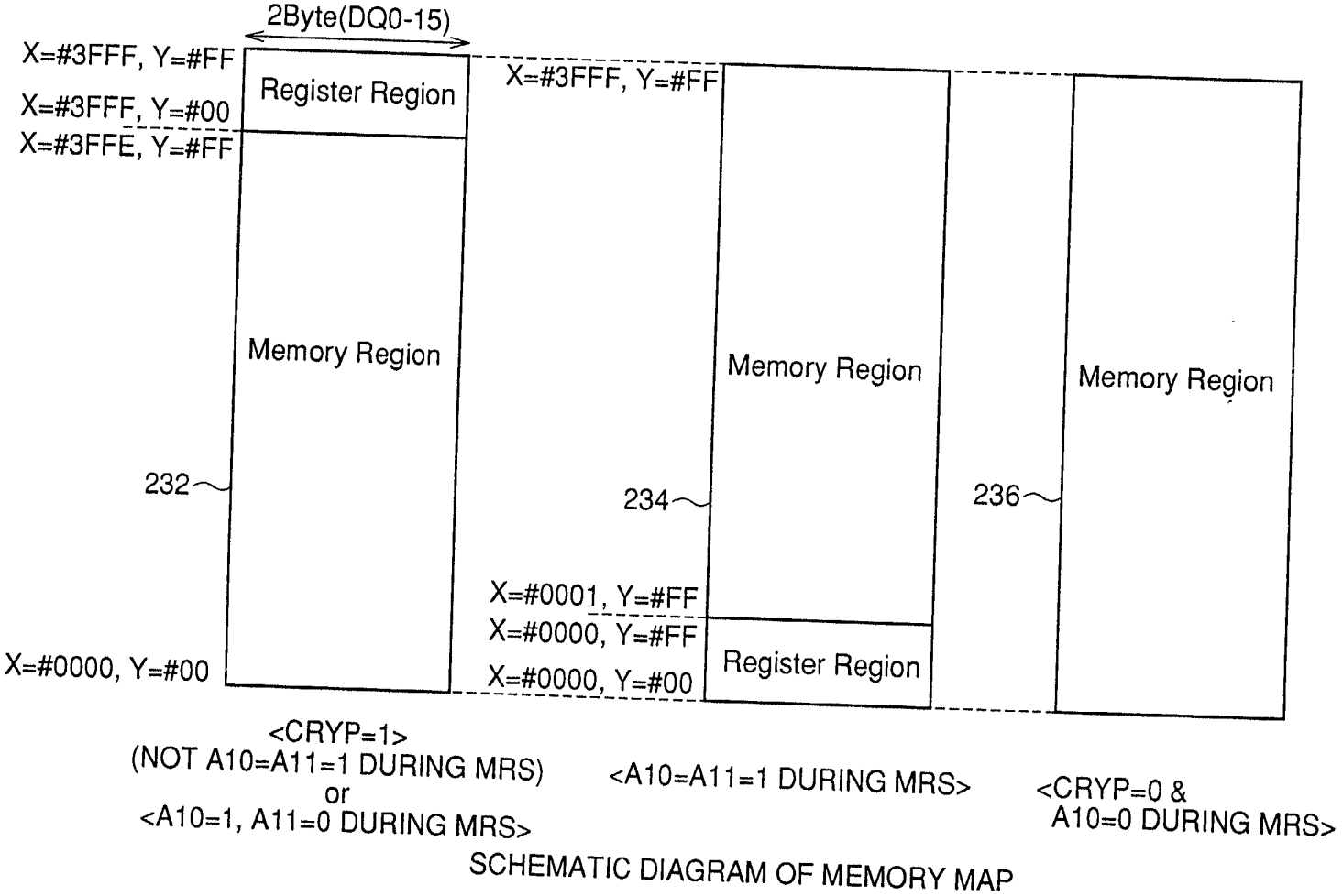

200
REG0
I/O DATA
REG1
INPUT DATA
SELECTOR
214
212
mbus[15:0]
CIPHER LOGIC
COUNTER
220
Reg, Logic, DRAM CONTROL
222
COUNTER
224
210
DRAM CONTROL ADDRESS COUNTER
I/O
Col Dec. & SA
Bank #0
EN/ DIS
mbus [15:0]
208
Mode reg.
REG2
OUTPUT DATA
204
206
228
202
CLK buff.
IO buff.
INPUT BUFFER
Row Dec.
CLK
DQ
ADD
CMD
CRYP

FIG.28



SCHEMATIC DIAGRAM OF MEMORY MAP

FIG.29

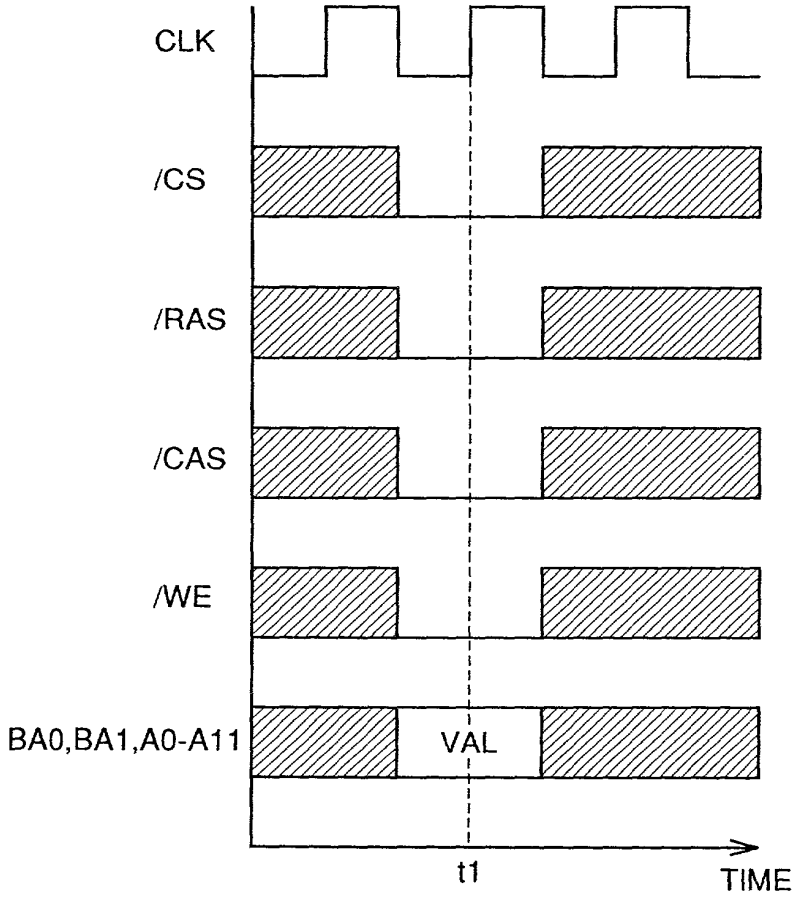


FIG.30

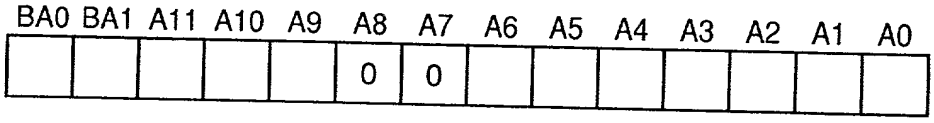


FIG.31

Bits	Name	Description	
A2..0	Burst Length	000 001 010 011 100 101 110 111	1 2 4 8 R R R Full Page
A3	Burst Type	0 1	Sequential Interleaved
A6..4	CAS Latency	000 001 010 011 1XX	R R 2 3 R
A9	Write Mode	0 1	Burst Single Bit
A10	Control Reg. Access	0 1	Disable Enable
A11	Control Reg. Address	0 1	X=3FFF X=0
BA1	Low Power Mode	0 1	Disable Enable
BA0	Low Clock Frequency	0 1	Disable Enable

FIG.32

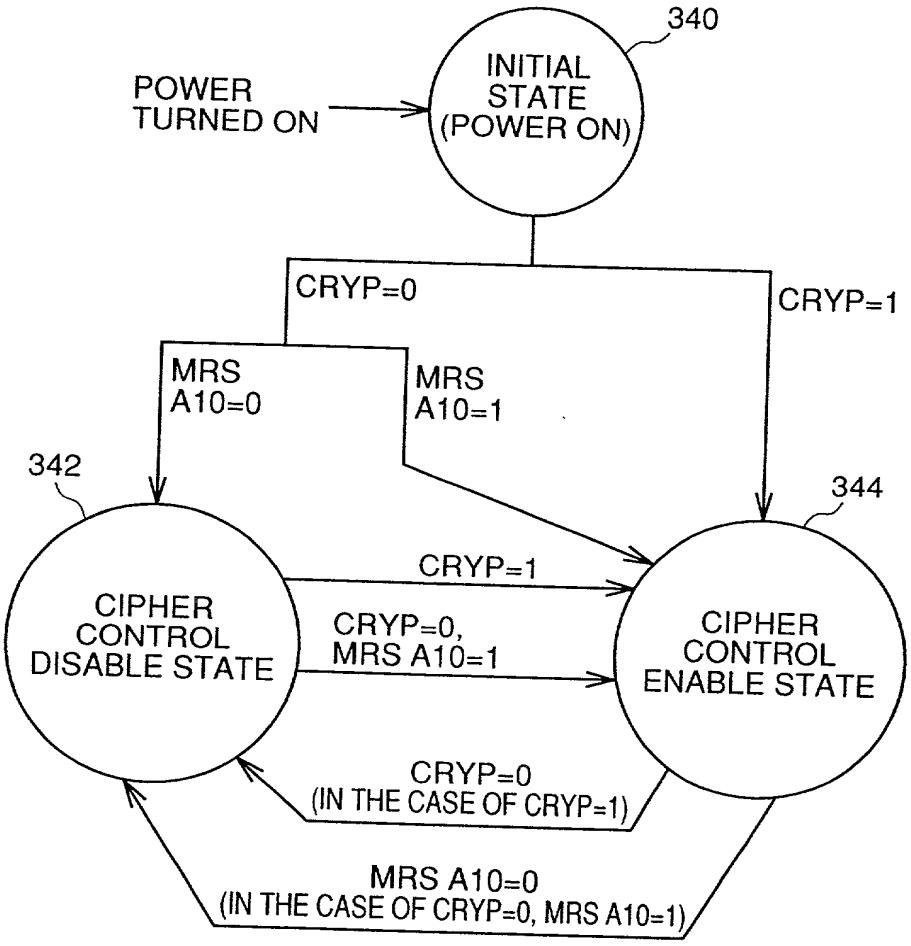

340
INITIAL STATE (POWER ON)
POWER TURNED ON
CRYP=0
CRYP=1
MRS A10=0
MRS A10=1
342
344
CRYP=1
CIPHER CONTROL DISABLE STATE
CRYP=0, MRS A10=1
CIPHER CONTROL ENABLE STATE
CRYP=0 (IN THE CASE OF CRYP=1)
MRS A10=0 (IN THE CASE OF CRYP=0, MRS A10=1)

FIG.33

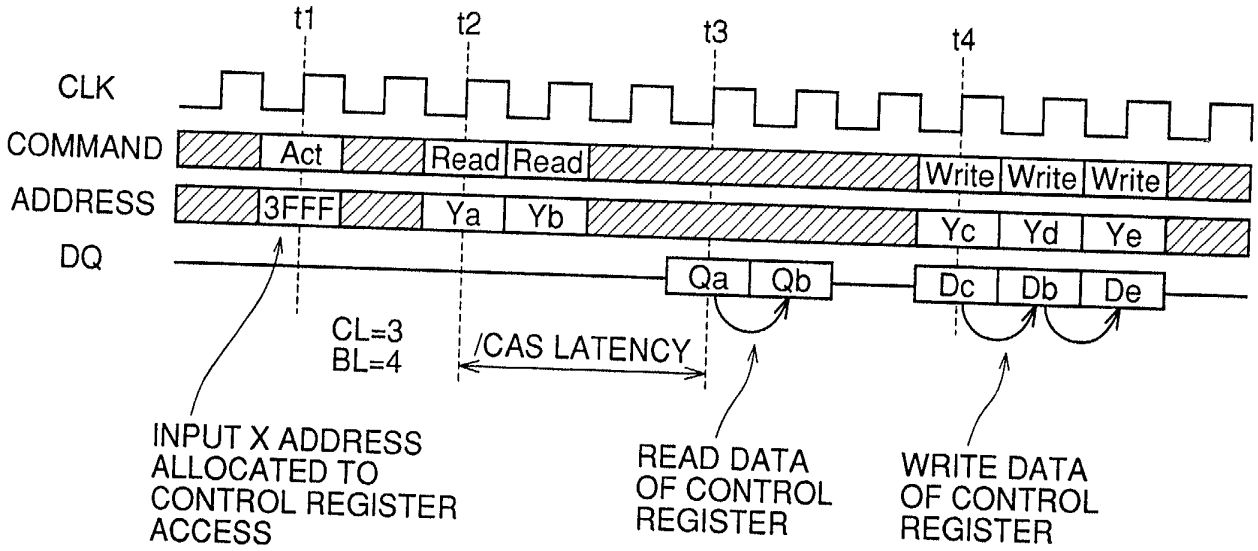

t1
t2
t3
t4
CLK
COMMAND
ADDRESS
DQ
Act
Read
Read
Write
Write
Write
3FFF
Ya
Yb
Yc
Yd
Ye
Qa
Qb
Dc
Db
De
CL=3
BL=4
/CAS LATENCY
INPUT X ADDRESS ALLOCATED TO CONTROL REGISTER ACCESS
READ DATA OF CONTROL REGISTER
WRITE DATA OF CONTROL REGISTER

FIG.34

Col. Add.	Bits	Name	Description		Access
h00	D0	Software Reset	1	Reset	W
	D1	Flag	0	Done	R
			1	Processing	R
	D2	Change add for reg. cont.	1	X=h3FFF	W
	D3	Change add for reg. cont.	1	X=h0	W
	D4	EOF(End of File)	1		W
h01	D1	Partial Refresh	1/0	Bank0 Enable/Disable	W
	D2		1/0	Bank1 Enable/Disable	W
	D3		1/0	Bank2 Enable/Disable	W
	D4		1/0	Bank3 Enable/Disable	W
	D5	LP Mode	1/0	Enable/Disable	W
	D6	Low Clock Frequency	1/0	Enable/Disable	W

FIG.35

Col. Add.	Bits	Name	Description		Access
h02	D1..0	Secret Cryp. Mode	00	Hold	W
			01	DES-56	W
			10	Triple DES-112	W
			11	Triple DES-168	W
	D5..2	Block Cryp. Mode	0000	Hold	W
			0001	ECB	W
			0010	CBC	W
			0100	OFB	W
			1000	CFB-64	W
	D9..6	Enabled bank set in	0000	All Bank Disable	W
	D6	Reg-DRAM transfer mode	1/0	Bank0 Enable/Disable	W
	D7		1/0	Bank1 Enable/Disable	W
	D8		1/0	Bank2 Enable/Disable	W
	D9		1/0	Bank3 Enable/Disable	W
	D10	Simulatenous transfer	1/0	Enable/Disable	W

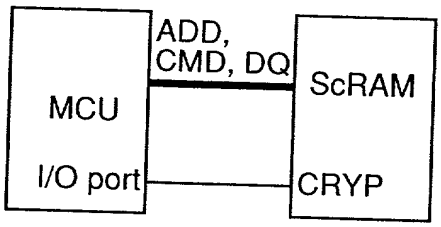
FIG.36

Col. Add.	Bits	Name	Description		Access
h03	D1..0	ENC/DEC	00	Hold	W
			01	Encryption	W
			10	Decryption	W
			11	RFU	W
	D2	Counter of reg1	1	Reset	W
	D3	Counter of reg2	1	Reset	W
	D4	IV Load	0	Previous output	W
			1	IV Load	W
	D8..5	Text length per block	0000	Hold	W
			Else	(D8..5)x1Byte	W
h04	D15..0	Reg.1 Access	-	Write Data: D15..0	W
h05	D15..0	Reg.2 Access	-	Read Data: D15..0	R
h06	D0	Reg-DRAM transfer	1	Mode entry	W
	D1		1	Mode exit	W
	D2		1	Counter reset of reg1	W
	D3		1	Counter reset of reg1	W

FIG.37

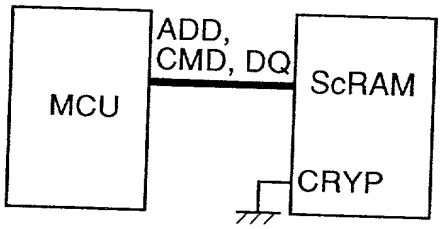
Col. Add.	Bits	Name	Description		Access
h13-h10	D15..0	Key1 for DES, Triple DES	LSB: h10[D0] USB: h13[D15]	Key1 Input	W
h17-h14	D15..0	Key2 for Triple DES	LSB: h14[D0] USB: h17[D15]	Key2 Input	W
h1B-h18	D15..0	Key3 for Triple DES-168	LSB: h18[D0] USB: h17B[D15]	Key3 Input	W
h1F-h1C	D15..0	Initial Vector (IV)	LSB: h1C[D0] USB: h1F[D15]	IV Input	W
hFF-h20	D15..0	Reserved			

FIG.38



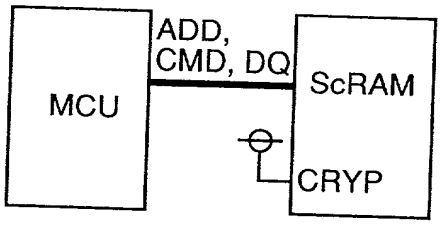
CONTROL CRYP TERMINAL BY I/O PORT

FIG.39



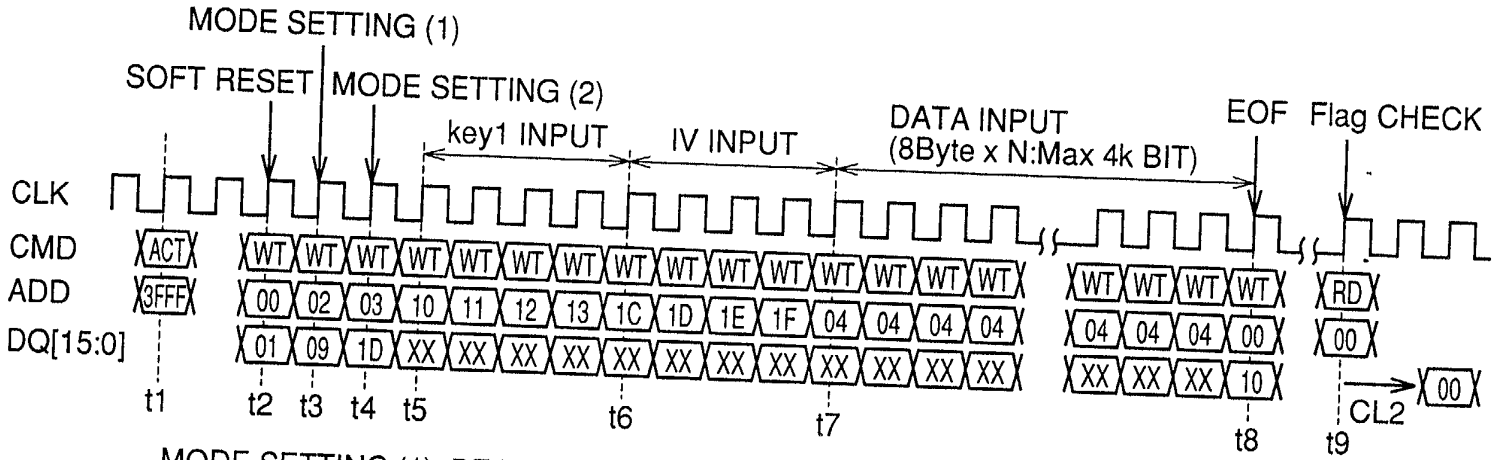
FIX CRYP TERMINAL AT L

FIG.40



FIX CRYP TERMINAL AT H

FIG.41



MODE SETTING (1): DES-56,CBC MODE
MODE SETTING (2): ENCRYPTION, RESET ADDRESS COUNTERS OF Reg1, 2, IV LOAD

FIG.42

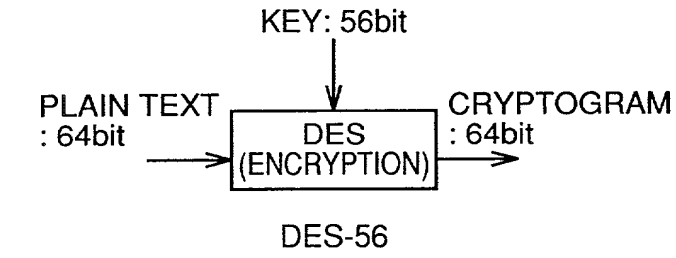


FIG.43

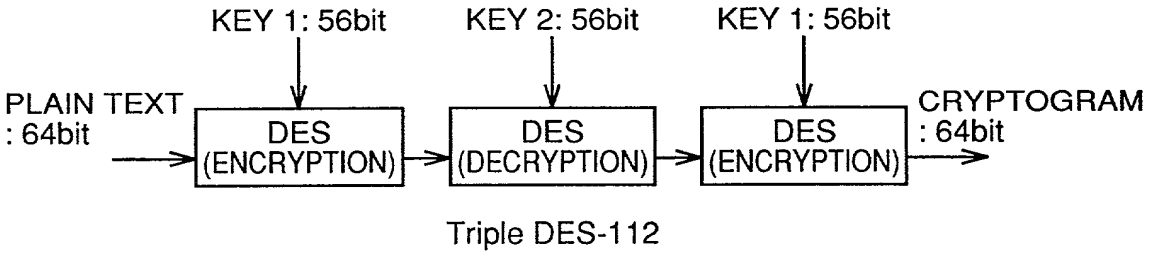


FIG.44

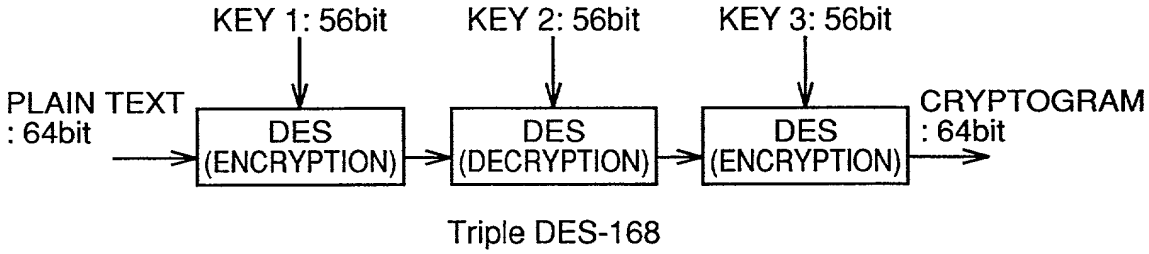


FIG.45

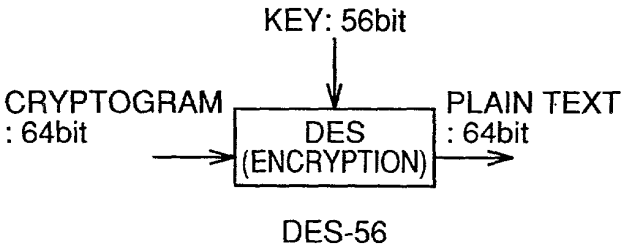


FIG.46

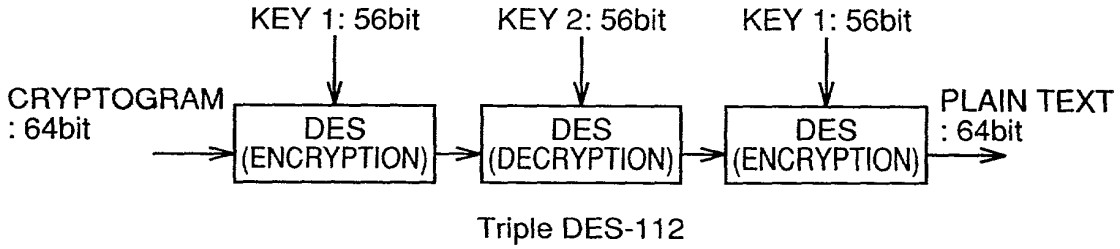


FIG.47

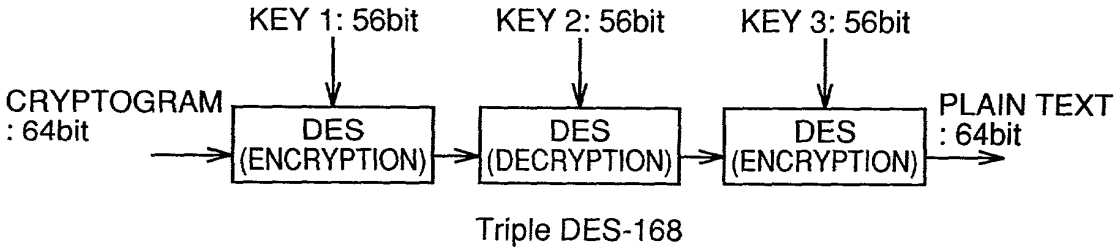


FIG.48

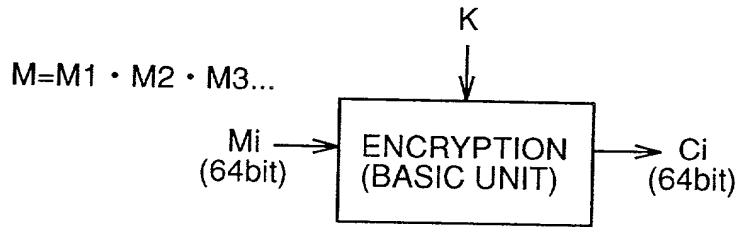


FIG.49

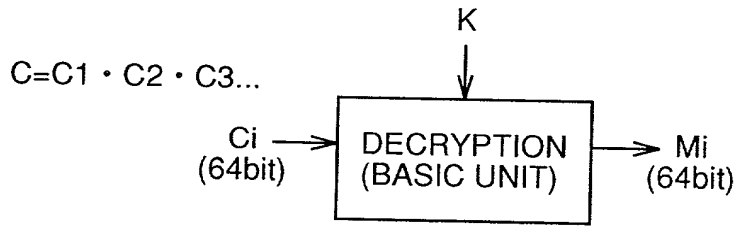


FIG.50

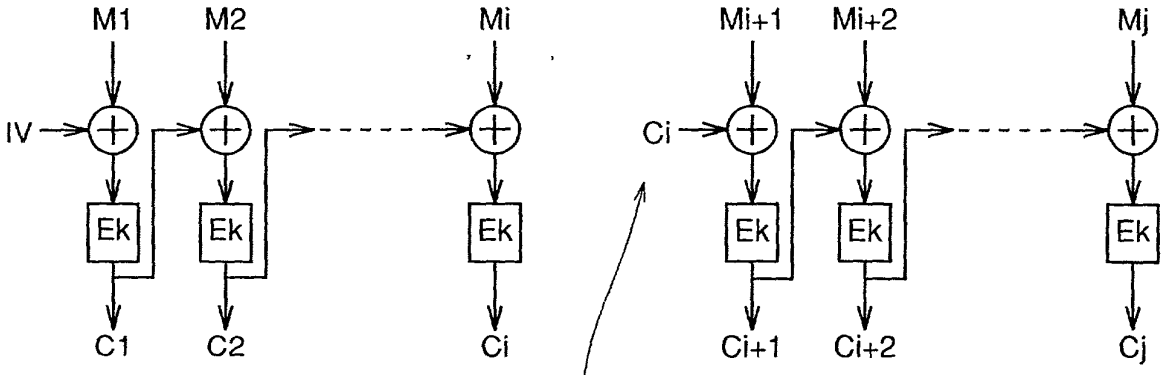
$C1 = Ek\ (M1 \oplus IV)$

$Ci = Ek\ (Mi \oplus Ci\text{-}1) \quad (i=2,3,.....)$

$M1 = Dk\ (C1) \oplus M1$

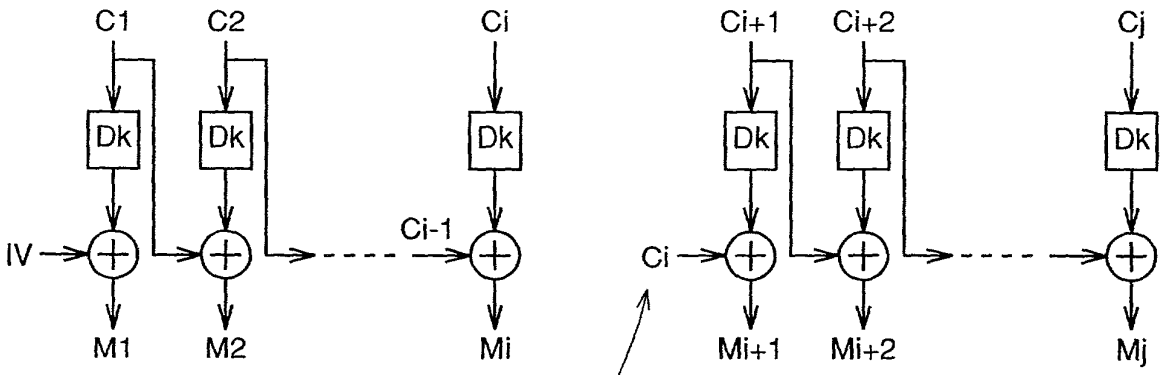
$Mi = Dk\ (Ci) \oplus Ci\text{-}1 \quad (i=2,3,.....)$

FIG.51



〈SCHEMATIC DIAGRAM OF ENCRYPTION IN CBC MODE〉

FIG.52



〈SCHEMATIC DIAGRAM OF DECRYPTION IN CBC MODE〉

FIG.53 PRIOR ART

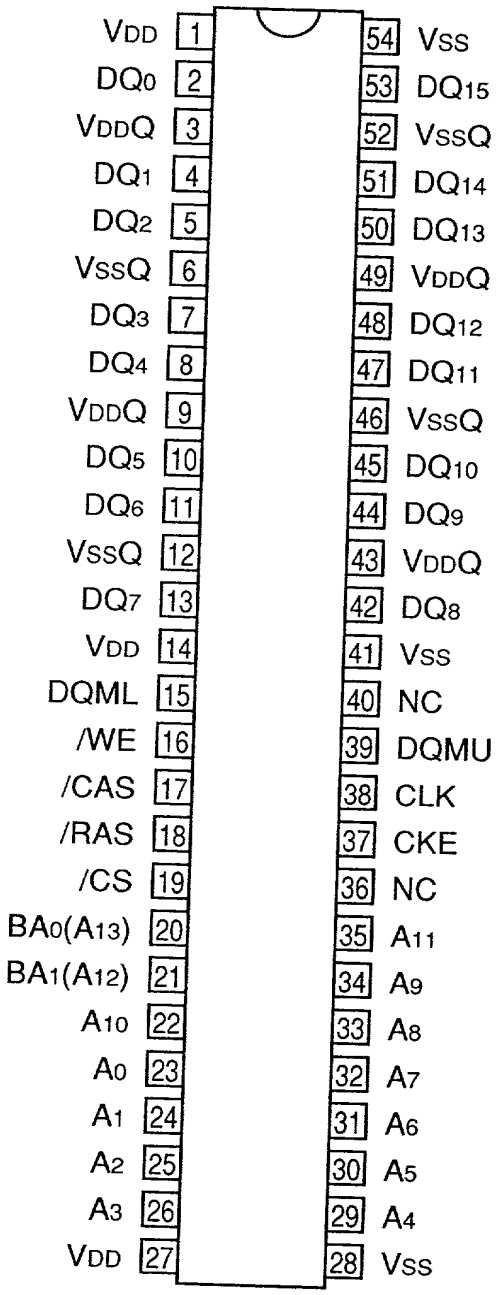


FIG.54 PRIOR ART

TERMINAL NAME	FUNCTION
CLK	MASTER CLOCK
CKE	CLOCK ENABLE
/CS	CHIP SELECT
/RAS	ROW ADDRESS STROBE
/CAS	COLUMN ADDRESS STROBE
/WE	WRITE ENABLE
$DQ_{0\sim15}$	DATA INPUT/OUTPUT
DQM(U/L)	OUTPUT DISABLE/WRITE MASK
$A_{0\sim11}$	ADDRESS INPUT
$BA_{0,1}(A_{12,13})$	BANK ADDRESS
V_{DD}	POWER SUPPLY POTENTIAL
$V_{DD}Q$	POWER SUPPLY POTENTIAL FOR OUTPUT
V_{SS}	GROUND
$V_{SS}Q$	GROUND FOR OUTPUT

FIG.55 PRIOR ART